RSA

Enc, Dec 실습

KeyGen

p, q : pick 1024 bits prime

N = p*q

φ(N) = (p-1)*(q-1)

e : pick random number(3으로 고정)

d : inverse e

pk := (N,e)

sk := d

return (N, e, d)

<Inverse e 구하는 방법>

단, e 와 φ(N)는 서로소

Ext-Euclid(e, φ(N)) = (1,x',y')

d = x' mod φ(N)

※

(e * d + φ(N)*y') mod φ(N) = 1 mod φ(N)

Enc(m,pk)

c = m^e mod n

return c

Dec(c,sk)

m = c^d mod n

return m